CSIRT.SK

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

MESAČNÁ SPRÁVA

JANUÁR 2026

TLP: CLEAR

Kybernetickým priestorom v januári 2026 rezonovalo hneď niekoľko kľúčových udalostí a útokov. Doplňujúce informácie môžete nájsť v časti Významné udalosti vo svete.

1 Spojené kráľovstvo spúšťa plán na posilnenie kyberobrany verejného sektora

Spojené kráľovstvo oznámilo nový kybernetický plán „Government Cyber Action Plan“ s viac než £210 miliónovým balíkom na posilnenie kybernetickej obrany verejného sektora, cieľom ktorého je zvýšiť odolnosť online služieb voči narušeniam, zlepšiť dohľad nad kybernetickými rizikami a koordinovať reakcie na incidenty pomocou novej Government Cyber Unit.

2 Spoločnosť Google sprístupnila Rainbow Tables na prelomenie hashov Net-NTLMv1

Stránka Google Research predstavila dataset Net-NTLMv1 Rainbow Tables, ktorý výskumníci a bezpečnostní analytici používajú na rýchle testovanie a lámanie zastaranej autentifikácie Net-NTLMv1 pomocou predpočítaných rainbow tabuliek s pevnou hodnotou výzvy (angl. challenge) 1122334455667788.

3 Útočníci zneužívajú nedostatočnú opravu zraniteľnosti na kompromitáciu zariadení Fortigate

Spoločnosť Arctic Wolf upozornila na automatické útoky na zariadenia Fortinet Fortigate, ktorých cieľom je vytvorenie nových používateľských účtov a exfiltrácia konfiguračných dát.

4 Kybernetický útok na sektor energetiky Poľska v decembri údajne zasiahol až 30 cieľov

V decembri 2025 koordinovaný kybernetický útok zasiahol približne 30 distribuovaných energetických zariadení (DER) v Poľsku. Analýza útoku je k dispozícii online.

5 MaaS platforma Stanley dokáže obísť bezpečnostné mechanizmy Chrome Web Store

Spoločnosť Varonis zverejnila informácie o novej službe malware-as-a-service s názvom Stanley, ktorá slúži na tvorbu škodlivých rozšírení pre Chrome a dokáže obísť bezpečnostné procesy Google a dostať tak malvér do obchodu Chrome Web Store.

6 Sofistikovaná phishingová kampaň cielená na Rusko infikuje systémy malvérom Amnesia Rat a ransomvérom

Útočníci spustili viacfázovú phishingovú kampaň zameranú na používateľov v Rusku, v ktorej najprv rozosielajú phishingové e-maily s podnikovými dokumentmi obsahujúcimi škodlivé skratky, ktoré pôsobia ako bežné súbory.

RIEŠENÉ INCIDENTY NA SLOVENSKU A Z NAŠEJ ČINNOSTI

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci január riešil typicky najmä phishingové kampane zasahujúce jeho konštituenciu. Vyskytli sa tiež prípady dlhodobo prebiehajúcej kampane, v ktorej útočníci v mene nadriadeného zamestnanca žiadajú obeť o informáciu o zostatku na účte organizácie. V podobných prípadoch jednotka v rámci analýzy vzorky preveruje možnosti získania bankových údajov podvodníkov, s ktorými následne osloví partnerov s požiadavkou o vykonanie príslušných procesov.

Tento mesiac sa opakovala podvodná smishingová kampaň impersonujúca Všeobecnú zdravotnú poisťovňu. Nahlasovateľ poskytol jednotke CSIRT.SK informácie a vzorky správ SMS/MMS. Útočníci cez ne šírili podvodnú doménu [vszp-obnova[.]com]. Po analýze a požiadaní o odstránenie obsahu predmetná URL prestala byť dostupná.

Vládna jednotka CSIRT riešila tiež prípad útoku na webovú stránku organizácie vo svojej konštituencii, pri ktorom prostredníctvom PHP súborov CMS WordPress získal útočník na ňu prístup. Následne vymazal súbory PHP, CSS, JavaScript, PDF a obrázky uložené na serveri. Útočník zmenil aj úvodnú stránku na podvodnú, ktorá sa tvárila, že overuje používateľov pomocou služby Cloudflare. Cieľom nového obsahu stránky bolo infikovať zariadenie používateľa malvérom. Na základe analýzy poskytnutých súborov bolo okrem iného identifikovaných viacero webshellov. Jednotka požiadala aj o informácie z logov, či v čase kompromitácie webu naň nepristupovala verejnosť. Organizácia obnovila stránku zo záloh.

Január sa niesol v duchu útočných kampaní na účty rôznych online služieb. Jedným z prípadov, ktoré jednotka CSIRT.SK riešila, boli zaznamenané pokusy o vytvorenie VPN pripojenia cez VPN koncentrátor s využitím slovníkových názvov používateľských účtov. Bezpečnostné systémy tieto pokusy eliminovali, pričom významne pomohlo aj nasadené viacfaktorové overovanie (MFA). Zasiahnutá organizácia po kontrole zistila, že nedošlo k prelomeniu účtov ani k prieniku do infraštruktúry. Jednotka organizácii poskytla odporúčania ako odolať predmetným útokom, resp. zabezpečiť ochranu proti opakovaným pokusom o prihlásenie.

V ďalšom prípade útokov na účty sa jednalo o slovníkový útok a útok hrubou silou na pracovné rozhranie s cieľom preniknúť do infraštruktúry dotknutej organizácie. Vzhľadom na bezpečnostné prvky v podobe dvojfaktorovej autentifikácie vo forme overovacích tokenov nedošlo k prieniku. Organizácia požiadala svojho poskytovateľa internetového pripojenia (ISP) o blokovanie dopytov pochádzajúcich zo zahraničia (geoip blokovanie). Po implementovaní opatrení pokusy o prienik ustali.

V rámci svojej proaktívnej činnosti jednotka CSIRT.SK vykonáva pravidelné skenovanie a overovanie zraniteľností v službách a zariadeniach IT infraštruktúr organizácií vo svojej konštituencii, ktoré sú vystavené do internetu. Využíva k tomu platformu Achilles, ktorú sama vyvíja a prevádzkuje. Systém Achilles slúži tiež na monitoring dostupnosti webových domén, ktorú monitoruje modul Domino.

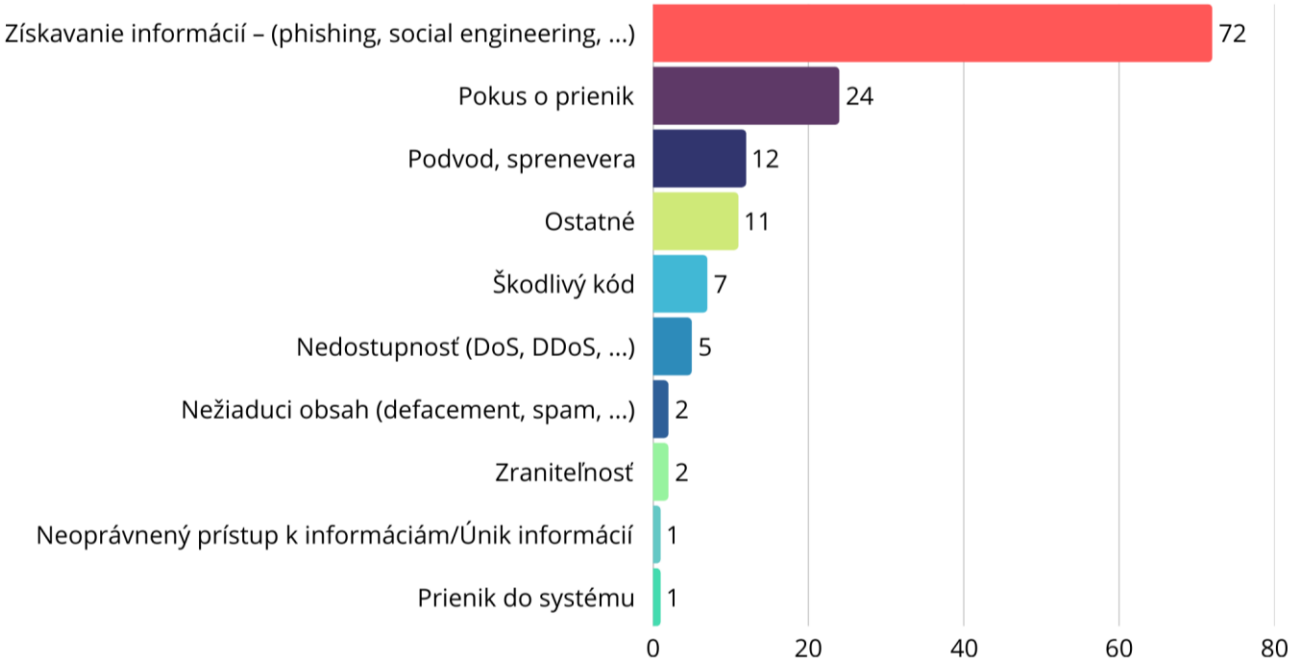
V rámci služby Ares boli vykonané 2 penetračné testy webových aplikácií. V rámci služby Afrodita prebiehal pravidelný monitoring hrozieb v kybernetickom priestore a zdieľanie indikátorov kompromitácie zo známych kampaní na ochranu vládnej siete Govnet.

V januári CSIRT.SK zaznamenala zvýšenú mieru útokov typu bruteforce/password guessing/password spraying na prihlasovacie rozhrania Fortinet SSL VPN a súvisiace služby, spojené pravdepodobne aj so

zneužívaním zraniteľnosti CVE-2026-24858. Preto plošne varovala svoju konštituenciu a poskytla odporúčania pre mitigovanie hrozby.

CSIRT.SK v rámci preventívnych činností organizuje aj vzdelávanie v oblasti kybernetickej bezpečnosti pre zamestnancov organizácií verejnej a štátnej správy, ako aj pre študentov stredných škôl. V januári jednotka prezentovala rôzne témy z oblasti kybernetickej bezpečnosti pre študentov Strednej priemyselnej školy stavebnej a geodézie v Bratislave.

VJ CSIRT poskytuje tiež školenia a cvičenia pre svoju konštituenciu v rámci výcvikového a školiaceho strediska Kyberaréna.



VÝZNAMNÉ UDALOSTI VO SVETE

Počas Vianoc boli zachytené automatizované útoky na servery Adobe ColdFusion

Výskumníci spoločnosti Greynoise zaznamenali počas Vianoc 2025 skenovanie a automatizované zneužívanie zraniteľnosti serverov Adobe ColdFusion. Zaznamenané aktivity boli iniciované z 10 IP adries patriacich hostingovej spoločnosti CTG Server Limited v Japonsku. Útočníci zneužívali už známe zraniteľnosti CVE-2023-26359, CVE-2023-38205, CVE-2023-44353, CVE-2023-38203, CVE-2023-38204, CVE-2023-29298, CVE-2023-29300, CVE-2023-26347, CVE-2024-20767 a CVE-2023-44352. Po úspešnej kompromitácii systémov spúšťali škodlivý kód a exfiltrovali prihlasovacie údaje z /etc/passwords prostredníctvom vyhľadávaní JNDI.

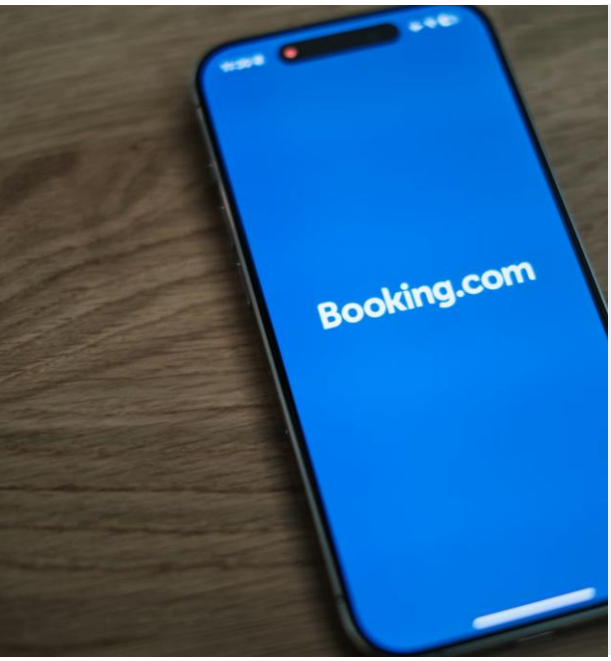
Útočníci zneužívajú Google Cloud Application Integration na rozposielanie phishingových správ

Spoločnosť Check Point upozornila na phishingovú kampaň zneužívajúcu službu Application Integration v Google Cloud. Útočníci rozosielali e-maily z legitímnej adresy noreply-application-integration@google.com, ktoré napodobňovali upozornenia na hlasové správy či zdieľané súbory. Vďaka odosielaniu z domén Google dokázali obchádzať DKIM, DMARC a SPF. Správy presmerovali používateľov na stránky s falošnou CAPTCHA na filtrovanie bezpečnostných nástrojov a následne na phishingovú stránku imitujúcu prihlasovanie do služieb Microsoft. Google prijal opatrenia proti zneužívaniu. Výskumníci z Xorlab a RavenMail zároveň zaznamenali aj OAuth phishing, ktorý po udelení oprávnení umožňuje prístup do cloudovej infraštruktúry Azure.

IAB broker Zestix kompromituje a predáva údaje z podnikových inštancií ShareFile, Nextcloud a OwnCloud

Platforma Hudson Rock informovala o aktivitách IAB (Initial Access Broker) skupiny Zestix súvisiacich s predajom citlivých údajov získaných z podnikových inštancií ShareFile, Nextcloud a OwnCloud. Systémy bez MFA boli napadnuté pomocou prihlasovacích údajov získaných infostealermi RedLine, Lumma a Vidar z infikovaných zariadení zamestnancov. Tieto škodlivé nástroje, šírené najmä cez malvertising a phishing, kradnú prihlasovacie údaje a kryptografický materiál z prehliadačov, komunikačných aplikácií či kryptopeňaženiek, pričom útočníci ich často okamžite zneužívajú. Pri podozrení na únik je nevyhnutná rotácia kryptografického materiálu, kontrola aktívnych relácií a zariadení a dôsledné využívanie viacfaktorovej autentifikácie.

VÝZNAMNÉ UDALOSTI VO SVETE

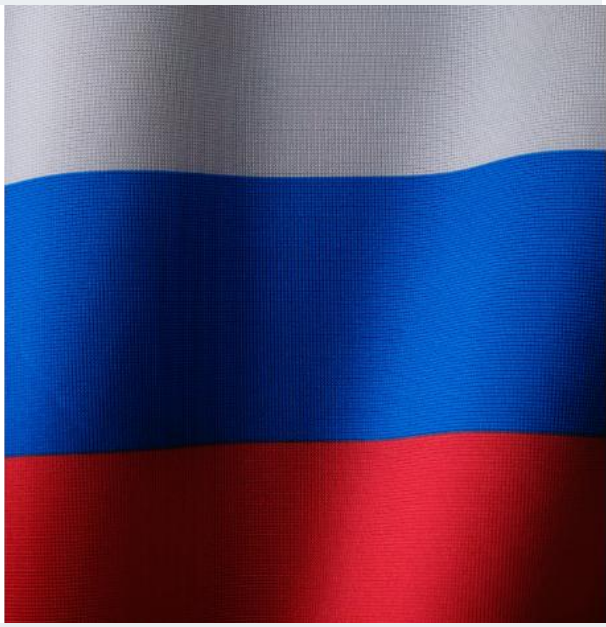


Kampaň ClickFix s tematikou Booking zobrazuje falošné obrazovky BSOD a šíri malvér DCRat

Spoločnosť Securonix informovala o phishingovej kampani ClickFix (PHALT#BLYX) zameranej na obete v Európe, ktorá od decembra 2025 šíri malvér DCRat. E-maily s témou zrušenia rezervácie na Booking.com presmerujú obeť na falošnú stránku s chybovým hlásením a následne zobrazia falošný Windows BSOD s pokynom spustiť škodlivý príkaz. PowerShell skript otvorí podvodnú stránku Booking.com na odpútanie pozornosti, zatiaľ čo na pozadí stiahne a cez MSBuild.exe skompiluje škodlivý .NET projekt, pridá výnimku do Defendera, vyžiada UAC oprávnenia a cez BITS stiahne finálny payload. Pre perzistenciu vytvorí .URL súbor v priečinku Startup. DCRat následne odosiela fingerprint zariadenia na C2 server a umožňuje ďalšie škodlivé operácie.

Prorusky orientovaná skupina UAC-0184 distribuuje Remcos RAT prostredníctvom Viber

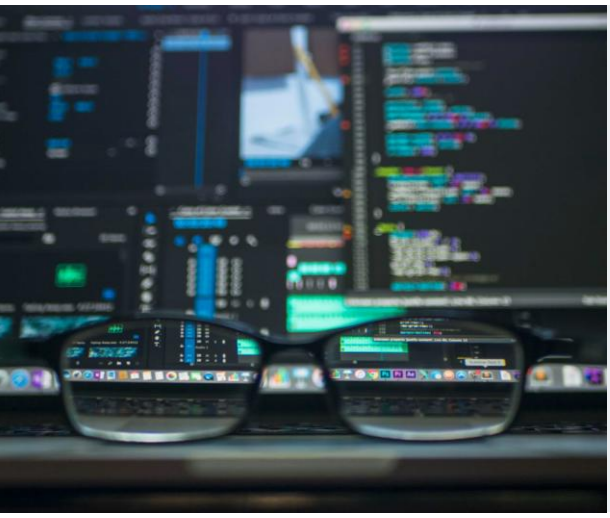
360 Advanced Threat Research Institute zverejnil analýzu útokov proruskej skupiny UAC-0184 na vládne a vojenské ciele Ukrajiny, pri ktorých šíri škodlivé ZIP archívy cez platformu Viber. Archívy obsahujú LNK súbory maskované ako dokumenty Word alebo Excel, ktoré po otvorení zobrazia návnadu a cez PowerShell na pozadí stiahnu ďalší škodlivý ZIP. Následne je pomocou DLL side-loading a module stomping nasadený Hijack Loader, ktorý vykoná fingerprinting, zabezpečí perzistenciu a spustí malvér Remcos RAT (Remote Access Tool). Na phishingové aktivity skupiny zneužívajúcej platformy Signal a Telegram upozornila CERT-UA už v januári 2024 a pokračujú dodnes.



Spojené kráľovstvo spúšťa plán na posilnenie kybernetickej obrany verejného sektora

Spojené kráľovstvo oznámilo nový plán „Government Cyber Action Plan“ s viac než £210 miliónovým balíkom na posilnenie kybernetickej obrany verejného sektora. Jeho cieľom je zvýšenie odolnosti verejných online služieb voči narušeniu, zlepšenie dohľadu nad rizikami v oblasti kybernetickej bezpečnosti a koordinovanie reakcie na incidenty pomocou novej jednotky Government Cyber Unit. Plán zavádza minimálne bezpečnostné štandardy, lepšiu viditeľnosť hrozieb a skúsenosti s incidentmi naprieč vládnymi oddeleniami a zahŕňa aj Software Security Ambassador Scheme. Toto opatrenie nadväzuje na novú legislatívu, ktorá má ešte viac posilniť obranu kritickej infraštruktúry a verejných služieb pred kybernetickými útokmi.

VÝZNAMNÉ UDALOSTI VO SVETE

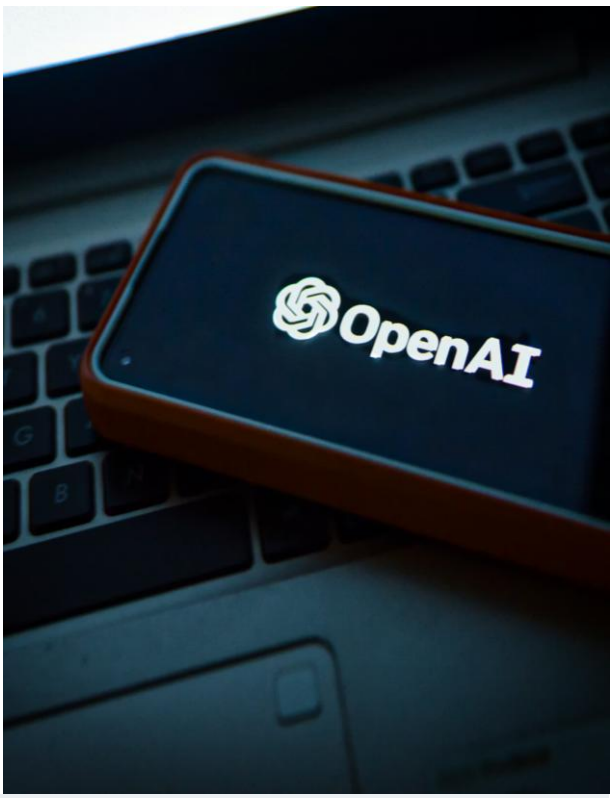


Únik databázy fóra BreachForums odkrýva 324 000 účtov

Platforma BreachForums utrpela únik údajov, pri ktorom sa na verejnosť dostali informácie približne 324 000 používateľských účtov, vrátane používateľských mien, e-mailových adries, hašovaných hesiel a ďalších technických informácií. K úniku došlo po tom, čo útočníci získali prístup k databáze fóra, ktoré už v minulosti čelilo viacerým zásahom zo strany OČTK. Incident opäť poukázal na riziká aj pre samotné komunity, ktoré sa venujú kriminálnej činnosti v oblasti kybernetickej bezpečnosti.

OpenAI spustila zobrazovanie reklamného obsahu v rámci odpovedí ChatGPT

Spoločnosť OpenAI spustila funkciu pre zobrazovanie reklamného obsahu v rámci odpovede vo verziách ChatGPT Free a ChatGPT Go. Lacná verzia predplatného ChatGPT Go za mesačný poplatok 8 dolárov v porovnaní s modelom ChatGPT Free poskytuje 10-násobne vyššie limity počtu správ, nahrávaní súborov, generovania obrázkov a umožňuje dlhšie držanie histórie a kontextu. Model ChatGPT Go však neposkytuje prístup k pokročilejším funkciám ako Thinking a Reasoning. V súvislosti s obavami so zavedením zobrazovania reklám spoločnosť OpenAI zdôraznila, že nemajú žiaden vplyv na odpovede ChatGPT, sú jasne a zrozumiteľne oddelené od odpovedí a obsah konverzácie nie je zdieľaný s tvorcami reklamného obsahu. Reklamy sa nesmú zobrazovať v blízkosti citlivých tém, ako je zdravie, politika alebo duševné zdravie. Predplatné programy ChatGPT PLUS, PRO, BUSINESS a ENTERPRISE nebudú obsahovať reklamy. Spoločnosť zavedenie reklám zdôvodnila potrebou získania dodatočných prostriedkov pre financovanie vývoja AGI (Artificial General Intelligence).



GOOGLE sprístupnili rainbow tables na prelomenie NET-NTLMv1 hashov

Stránka Google Research predstavila dataset Net-NTLMv1 Rainbow Tables, ktorý výskumníci a bezpečnostní analytici používajú na rýchle testovanie a lámanie zastaranej autentifikácie Net-NTLMv1 pomocou vopred vypočítaných dúhových tabuliek (angl. rainbow tables) s pevnou hodnotou výzvy (angl. challenge) 1122334455667788. Dataset slúži na demonštráciu, ako ľahko útočníci dokážu získať heslá zo zachytených hašov, a tým upozorňuje organizácie na potrebu vypnúť Net-NTLMv1 a prejsť na modernejšie a bezpečnejšie mechanizmy overovania.

VÝZNAMNÉ UDALOSTI VO SVETE

Nová verzia Cybersecurity Act posilňuje kybernetickú bezpečnosť v EÚ a zavádza možnosť obmedzenia až úplného zákazu technológií

Európska Komisia predložila návrh novej verzie Cybersecurity Act, ktorá prináša viacero noviniek, vrátane možnosti nariadiť odstránenie produktov vysokorizikových dodávateľov z telekomunikačných sietí. Tento krok by mal zvýšiť odolnosť prvkov kritickej infraštruktúry pred útokmi kyberkriminálnych skupín a štátmi sponzorovaných útočníkov. Čiastočne ide o reakciu na rôznu mieru praktickej implementácie 5G Security Toolboxu, ktorý členské štáty nabádal k limitovaniu využívania rizikových produktov. Návrh zatiaľ neobsahuje špecifikáciu konkrétnych technológií, avšak EÚ dlhodobo upozorňuje na produkty čínskych technologických gigantov Huawei a ZTE. Nový zákon by komisii umožnil vykonávať analýzu rizík na úrovni EÚ a zavádzať obmedzenia alebo úplný zákaz vybraných produktov v rámci kritickej infraštruktúry. Novela zákona tiež podporuje proces certifikácie spoločností, dáva agentúre ENISA možnosť vydávať varovania a vystupovať v roli jednotného bodu pre hlásenie kybernetických incidentov a zlepšuje možnosti spolupráce s Europolom. Návrh zákona vstúpi do platnosti po jeho schválení Európskym parlamentom a Radou EÚ.

Platforma MaaS Stanley dokáže obísť bezpečnostné mechanizmy Chrome Web Store

Spoločnosť Varonis upozornila na malware-as-a-service platformu Stanley na tvorbu škodlivých rozšírení pre Google Chrome, ktorá dokáže obísť bezpečnostné procesy a dostať malvér do Chrome Web Store. Na hackerských fórach ju promuje používateľ vystupujúci pod aliasom Stanley. Rozšírenia pre Chrome, Edge a Brave monitorujú webové stránky zobrazované v prehliadači a cez iframe ich prekryjú phishingovým obsahom bez zmeny URL. Podporujú aj push notifikácie, ktoré možno zneužiť na agresívnejšie šírenie phishingu. Platforma taktiež umožňuje fingerprinting a filtrovanie obetí na báze IP adresy, geolokácie a korelácie medzi reláciami a zariadeniami. Zdrojový kód obsahuje viacero nedokončených častí a komentáre v ruštine. Platforma však poukazuje na princíp „v jednoduchosti je krása“. Unikátne je hlavne obchádzanie procesov revízie, ku ktorým sa spoločnosť Google zatiaľ nevyjadrila. Na problémy s procesom revízie, umožňujúce pridanie škodlivých rozšírení, upozornili aj výskumníci spoločností Symantec a LayerX. Vo všeobecnosti platí pravidlo, že by používatelia mali obmedziť množstvo používaných modulov a inštalovať len tie od dôveryhodných vývojárov a s dobrou reputáciou. V prípade sofistikovaných útokov na dodávateľský reťazec však ani tieto opatrenia nepostačujú.

VÝZNAMNÉ UDALOSTI VO SVETE


Designed by Freepik

Útočníci aktívne zneužívajú nedostatočnú opravu zraniteľnosti CVE-2025-59718 na kompromitáciu zariadení Fortinet Fortigate

Spoločnosť Arctic Wolf upozornila na automatické útoky na zariadenia Fortinet Fortigate, ktorých cieľom je vytvorenie nových používateľských účtov a exfiltrácia konfiguračných dát. Kampaň je aktívna minimálne od 15. januára 2026 a útočníci zneužívajú bližšie nešpecifikovanú zraniteľnosť v službe SSO (Single Sign On) na vytváranie nových účtov s VPN prístupom a následný export konfigurácie. Aktivita vykazuje vysokú mieru podobnosti s útokmi založenými na zneužití zraniteľnosti CVE-2025-59718 v produktoch spoločnosti Fortinet v decembri 2025. Túto bolo možné zneužiť na zariadeniach s aktívnou FortiCloud SSO zaslaním špeciálne vytvorených správ SAML na obídenie mechanizmov autentifikácie. Nedávno používatelia produktov Fortinet taktiež informovali o útokoch spojených s nedostatočnou opravou tejto zraniteľnosti v rámci aktualizácií z decembra, ktorú mal údajne potvrdiť aj samotný výrobca Fortinet.

Kybernetický útok na sektor energetiky Poľska v decembri 2025 údajne zasiahol až 30 cieľov

V decembri 2025 zasiahol koordinovaný kybernetický útok približne 30 distribuovaných energetických zariadení (DER) v Poľsku. Útočníci kompromitovali operačné technológie (OT) a poškodili kľúčové zariadenia tak, že ich nebolo možné obnoviť, pričom energetická výroba zostala bez výpadku. Bezpečnostná spoločnosť Dragos útoky pripisuje ruskej skupine Electrum, ktorá síce zdieľa TTP s APT44 (Sandworm), ale podľa výskumníkov vykonáva odlišnú množinu aktivít. Spoločnosť ESET útoky pripisuje ruskej štátom sponzorovanej skupine APT44, ktorá pri nich mala použiť nový malvér DynoWiper.


Designed by Freepik

Európska komisia vyšetruje Grok za generovanie deepfake obrázkov so sexuálnou tematikou

Európska komisia v súvislosti s možnosťou využitia AI nástroja Grok od platformy X na generovanie obrázkov so sexuálnou tematikou začala vyšetrovanie služby v zmysle porušenia nariadenia DSA (Digital Services Act). Služba má údajne umožňovať generovanie sexuálneho deepfake obsahu zobrazujúceho ženy a deti. Grok v rovnakej veci vyšetruje aj britský komunikačný regulačný orgán Ofcom a štát Kalifornia. Platforma X vyhlásila, že generovanie obrázkov s danou tematikou zablokuje a prístup k službe obmedzí len na platiacich používateľov.

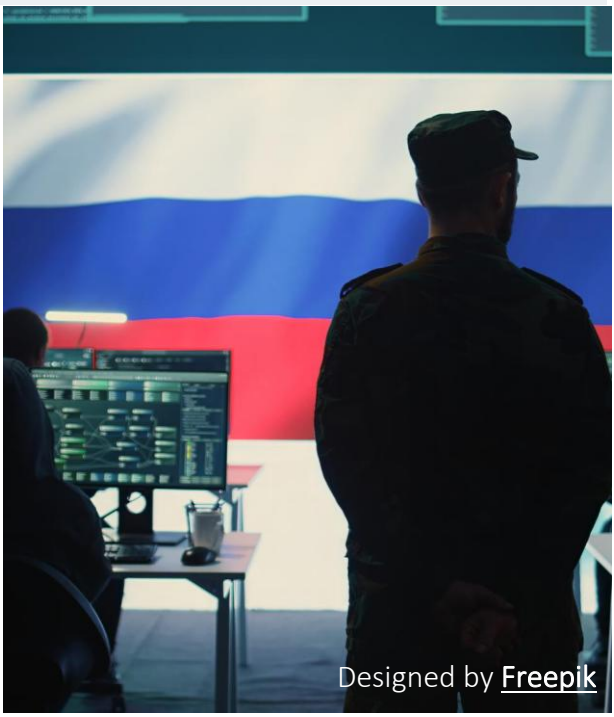
VÝZNAMNÉ UDALOSTI VO SVETE

Vydieračská skupina ShinyHunters pokračuje vo vishingových útokoch v mene IT podpory

Skupina ShinyHunters tvrdí, že stojí za vlnou hlasových phishingových útokov, pri ktorých útočníci telefonicky kontaktujú zamestnancov a predstierajú, že sú IT podpora. Touto cestou sa snažia získať ich prihlasovacie údaje a kódy MFA pre SSO účty na platformách ako Okta, Microsoft Entra či Google. Kompromitované SSO účty im potom umožnia pristupovať k prepojeným firemným aplikáciám a službám. Útočníci exfiltrujú citlivé dáta, ktoré používajú na vydieranie firiem. Skupina potvrdila svoju účasť na niektorých z týchto podvodných kampaní a uviedla, že sa prednostne zameriava na spoločnosť Salesforce.

Sofistikovaná phishingová kampaň cielená na Rusko systémy infikuje malvérom Amnesia RAT a ransomvérom

Útočníci spustili viacfázovú phishingovú kampaň zameranú na používateľov v Rusku, v ktorej najprv rozosielajú phishingové e-maily s podnikovými dokumentmi obsahujúcimi škodlivé skratky, ktoré pôsobia ako bežné súbory. Po ich otvorení deaktivujú bezpečnostné prvky Microsoft Defender, vykonávajú prieskum systému a manipulujú s politikami Windows, aby znefunkčnili ochranu. Následne nasadia malvér Amnesia RAT (remote access trojan) a ransomvér z rodiny Hakuna Matata, ktoré útočníkom umožnia ukradnúť dáta a získať trvalý prístup alebo poškodiť systémy. Táto komplexná kampaň ukazuje, ako moderné malvérové operácie kombinujú phishing, skripty a techniky na obchádzanie detekcie na dosiahnutie plnej kompromitácie cieľových zariadení.



VÝZNAMNÉ UDALOSTI VO SVETE

- Výskumníci upozornili na riziká aplikácií AI IDE súvisiace s ich odporúčaniami rozšírení neexistujúcimi na OpenVSX.
- Škodlivé rozšírenia pre Google Chrome exfiltrujú obsah konverzácií s AI.
- FBI varuje pre cielenými quishingovymi kampaňami severokórejskej skupiny Kimsuki.
- Španielsko zatklo 34 podozrivých z medzinárodnej kyberkriminálnej siete Black Axe.
- APT28 spustila kampaň na krádež prihlasovacích údajov v Európe a Ázii.
- Irán odpojil internet po celej krajine počas zásahu proti protestujúcim.
- Spoločnosť Anthropic predstavila modul Claude AI pre spracovanie zdravotných záznamov.
- Ruská skupina void Blizzard cieli na UA armádu prostredníctvom správ na WhatsApp a Signal, cez ktoré šíri malvér PLUGGYAPE.
- Platforma GrubHub potvrdil prienik do systémov a exfiltráciu dát.
- OČTK identifikovali vodcu ransomvérovej skupiny Black Basta a pridali ho na zoznamy Interpolu a Europolu.
- LastPass varuje zákazníkov pred prebiehajúcou phishingovou kampaňou.
- Európska únia spustila GCVE, decentralizovanú verejnú databázu zraniteľností ako alternatívu k americkému systému CVE.
- Microsoft predstavil novú funkciu Teams na detekciu podozrivých VoIP hovorov.
- WhatsApp zavádza režim lockdown pre vysokorizikových používateľov.
- V USA odsúdili slovenského občana za prevádzkovanie darknetového obchodu Kingdom Market.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Microsoft opravil dlhodobo zneužívanú vlastnosť súborov LNK

Spoločnosť Microsoft opravila v rámci novembrového Patch Tuesday vysoko závažnú zraniteľnosť súborov .LNK. Chyba umožňuje útočníkom zaviesť obeť a ukryť do súboru odkazu .LNK príkaz na vykonanie škodlivého kódu alebo skript. Zraniteľnosť je aktívne zneužívaná minimálne od roku 2017.

Kritická zraniteľnosť Cisco AsyncOS je aktívne zneužívaná

Vývojári Spoločnosť Cisco varovala pred aktívnym zneužívaním kritickej zero-day zraniteľnosti v produktoch Cisco SEG (Secure Email Gateway) a SEWM (Secure Email and Web Manager). Zraniteľnosť s identifikátorom CVE-2025-20393 v operačnom systéme AsyncOS umožňuje vzdialene vykonávať systémové príkazy a kompromitovať zraniteľný systém.

MongoBleed: aktívne zneužívaná zraniteľnosť umožňuje čítať pamäť

Vývojári MongoDB Server opravili vysoko závažnú zraniteľnosť umožňujúcu vzdialenému neautentifikovanému útočníkovi manipulovať premenné v hlavičkách požiadaviek a získavať tak citlivé informácie z pamäte na halde (angl. heap) v rámci operačnej pamäte. Zraniteľnosť je aktívne zneužívaná.

Platforma Coolify obsahuje 11 kritických zraniteľností

Vývojári open-source platformy pre manažovanie serverov, aplikácií a databáz Coolify opravili 11 kritických chýb, ktoré môžu viesť k obídeniu autentifikácie, vzdialenému vykonaniu kódu a úplnému kompromitovaniu hostiteľského systému. Chyby zabezpečenia súvisia najmä s neošetrenými parametrami, nad ktorými má kontrolu používateľ. Tieto aplikácia preberá priamo do príkazov pre shell.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Trend Micro Apex Central obsahuje tri závažné zraniteľnosti

Spoločnosť Trend Micro vydala bezpečnostné aktualizácie svojho produktu Apex Central pre Windows, ktoré opravujú 3 zraniteľnosti, z čoho 1 je označená ako kritická. Kritická zraniteľnosť umožňuje neautentifikovanému útočníkovi vykonávať vzdialene kód s oprávneniami úrovne SYSTEM. Ďalšie dve zraniteľnosti by mohol vzdialený neautentifikovaný útočník zneužiť na zneprístupnenie služby.

Zraniteľnosť NPM knižnice Binary-Parser umožňuje vzdialené vykonanie kódu

Vývojári NPM knižnice pre parsovanie binárnych dát binary-parser vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú kritickú zraniteľnosť CVE-2026-1245. Táto spočíva v nedostatočnom overovaní používateľských vstupov, čo by mohol vzdialený neautentifikovaný útočník zneužiť na vzdialené vykonanie kódu JavaScript s privilégiami procesu Node.js.

Kritické zraniteľnosti v NPM knižniciach jsPDF a AdonisJS

Bezpečnostní výskumníci našli kritické zraniteľnosti vo dvoch knižniciach NPM – jsPDF na generovanie PDF dokumentov a MVC knižnici AdonisJS. Ide o často využívané knižnice, ktoré majú spolu viac ako 3,5 milióna stiahnutí týždenne.

Kritická zraniteľnosť Fortinet FortiSIEM

Spoločnosť Fortinet opravila kritickú zraniteľnosť FortiSIEM, ktorá umožňuje kontrolovať obsah požiadaviek TCP a následne vykonávať kód a príkazy s oprávneniami administrátora, bez potreby autentifikácie.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Zraniteľnosť WP modulu umožňuje získanie administrátorskej kontroly

Vývojári modulu Advanced Custom Fields: Extended pre WordPress vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú kritickú zraniteľnosť. CVE-2025-14533 spočíva v nesprávnej reštrikcii rolí v rámci formulára pre tvorbu a editáciu používateľov. Vzdialený neautentifikovaný útočník by ju mohol zneužiť na získanie administrátorského prístupu a úplnej kontroly nad systémom.

Spoločnosť Cisco opravila kritickú zero-day zraniteľnosť v produktoch

Spoločnosť Cisco opravila kritickú aktívne zneužívanú zraniteľnosť CVE-2026-20045 vo viacerých svojich produktoch. Zraniteľnosť umožňuje neautentifikovanému útočníkovi vzdialene vykonávať systémové príkazy a získať oprávnenia používateľa root.

Telnetd obsahuje kritickú zraniteľnosť

Nástroj telnetd v balíku GNU InetUtils nesanitizuje používateľské vstupy v niektorých premenných. Tým umožňuje injektovať hodnoty vedúce k obídeniu autentifikácie a získanie prístupu s oprávneniami používateľa root. V nástroji sa nachádza vyše 10 rokov.

Zraniteľnosť vm2 pre Node.js umožňuje obísť sandboxing

Vývojári knižnice vm2 pre Node.js s funkcionalitou sandboxingu opravili kritickú chybu, ktorá útočníkom umožňuje uniknúť zo sandboxu a vykonávať ľubovoľný kód.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Fortinet opravil aktívne zneužívanú kritickú zraniteľnosť vo FortiCloud SSO

Spoločnosť Fortinet vydala bezpečnostné aktualizácie FortiOS, FortiManager, FortiProxy a FortiAnalyzer, ktoré opravujú aktívne zneužívanú kritickú zraniteľnosť vo FortiCloud SSO. CVE-2026-24858 by vzdialený neautentifikovaný útočník mohol zneužiť na obídenie autentifikácie na zraniteľné zariadenia.

MESAČNÍK ZRANITEĽNOSTÍ JANUÁR 2026

VJ CSIRT pravidelne vydáva mesačný prehľad kritických zraniteľností.

https://csirt.sk/posts/3104.html